Appendix E – Educational Technology Operating Norms

In addition to RFA Standard Terms and Conditions (Appendix A, Articles I&II), and Standards, Evaluation Criteria & Best Practices (Appendix D), and subject to periodic updates provided by the Chancellor's Office, the following operating standards, or "norms", shall be adopted and consistently executed by grantees and subgrantees performing technology related work funded by Chancellor's Office Program grants, contracts and agreements.

Each applicant must warrant within the application response that:

1. Applicant will adopt and implement all Edtech operating norms to fulfill program and project objectives.
2. Applicant's current organization and IT policies and protocols will enable them to successfully meet the expectations of the Edtech standards and controls as outlined in Appendix E.
   a) Where the applicant's current organizational structure or IT policies and protocols are insufficient to immediately meet Edtech standards and control requirements, the applicant has provided details for a realistic approach and timeline to resolve deficiencies.

Article I. Program & Project Structure

Section 1.01 Standard CCC Chancellor's Office (CCCCO) Roles & Engagement Expectations

(a) In addition to Grant Monitor(s), the CCCCO will assign CCCCO representatives to lead and oversee progress within each program and project funded through the CCCCO. The grantee and/or subgrantee is required to consistently engage and utilize CCCCO leaders for the entire duration of the program or project. CCCCO leadership role include, but are not limited to:

(b) Executive Sponsor

- *(i) Is usually a divisional Executive Vice Chancellor*
- *(ii) Is accountable for the success of the program or project*
- *(iii) Provides overarching strategic direction, has authority to make high risk/high impact decisions and large budgetary decisions, removes political barriers to success, and advocates for the program at national, state and system-wide levels*
- *(iv) Champions legislative change and steers system-wide organizational change management efforts*

(c) Sponsor(s)

- *(i) Is usually a divisional Vice Chancellor(s)*
  1) one represents Students, Faculty and/or Admin Staff, and
  2) one represents technology or data
- *(ii) Is responsible for the success of the program or project*
- *(iii) Interfaces and collaborates with and provides direction to grantee or subgrantee leadership roles*
- *(iv) Is responsible for assigning advisory committee membership from the field and co-facilitating advisory committee meetings*
- *(v) Drives strategic direction, has authority to make med-high risk/impact and budgetary decisions, removes political barriers to success, and advocates for the program at national, state and system-wide levels*
- *(vi) Reviews and approves system-wide program communications (both written and verbal) drafted by the CCCCO Lead and/or grantee/ subgrantee program manager*
- *(vii) Supports system-wide organizational change management efforts*

(d) Lead

- *(i) Is usually a divisional Dean representing Students, Faculty and/or Admin Staff, or technology or data*
- *(ii) Is responsible for direct engagement with grantee and subgrantee program and product managers to plan, execute and successfully deliver program and project outcomes*
- *(iii) Is responsible for identifying and engaging project working team members from the field and facilitating field engagement during the product development lifecycle*
- *(iv) Identifies risks and issues, and co-develops and executes mitigation strategies with grantee and/or subgrantee program and product managers*
- *(v) Has authority to make low to medium risk/impact decisions, removes political barriers to success, and advocates for the program and system-wide levels*

(vi) Drives system-wide organizational change management efforts

Section 1.02 Program Advisory & Steering Teams (Working Groups)

(i) The CCCCO will strive to keep advisory committee focus system-wide vs. program focused and keep membership, meetings and activities to realistic and reasonable levels and frequencies. See below for a list of CCCCO recognized advisory committees for Edtech Programs and projects:

1) Telecomm & Technology Advisory Committee (TTAC)
2) Field and Industry Team Advisory Committee (5 Cs)
   a) Meet Quarterly (either in person or remotely) for 8 hrs. or less
   b) Meet periodically (adhoc) via conference call or web meeting to discuss urgent matters for which advisory support is desired prior to the next scheduled meeting

(ii) Within Edtech programs and projects, steering teams or "working groups", will meet often to make tactical recommendations and define requirements as part of the project team

For example:

1) Sponsors – steer by driving strategic direction and making critical program decisions
2) Leads – steer by making final calls on product requirements and pilot and production go/no go decisions
3) Field SMEs – steer by defining low-level product requirements by role
4) Architects & engineers – steer by defining architectural and technical requirements
5) From time to time, a working group may be created to research and provide recommendations to the Advisory Committee(s)

(iii) The CCCCO Sponsor(s) must review and approve any request to form a program or project specific advisory committee or steering committee

Article II. Standards by Function

Section 2.01 Program and Project Staffing

(a) Grantees and subgrantees will employ a variable staffing model in order to flexibly adjust capacity based on periodic changes in strategy and funding. Any plan for hiring new full-time equivalent employees (PYs) must be submitted and approved in advance by the CCCCO Sponsor(s).

(b) All candidates for any in-scope role must demonstrate that they have the skill and experience to perform the work. Development roles can only be filled by employees, not contractors or consultants, as long as the grantee or subgrantee will provide the support and coaching required to ensure the employee develops quickly, and the workplan & project objectives are met.

(c) Grantees and subgrantees will engage CCCCO Sponsors and/or Leads to vet all prospective employees, contractors and consultants which are being considered for key leadership roles within the program and/or project. Key leadership roles can be classified as any role which will directly interface with Executive Vice Chancellors, Vice Chancellors, and/or Deans within the CCCCO, or with high-ranking stakeholders within advisory committees like Telecomm and Technology Advisory Committee (TTAC), including, but not limited to:

(i) Program Directors or Managers

(ii) Product Directors or Managers

(iii) Industry or Functional Experts

(d) CCCCO Sponsors and functional leaders will be given the option to participate in hiring/sourcing of key talent required by grantee program teams to ensure skill, capability and cultural fit.

(e) The CCCCO has the option to evaluate or assess the skills and capabilities of all grant funded resources to identify misalignment and gaps and/or develop and execute a focused employee training and talent sourcing plan.

(f) Anti-Lobbying – Key Talent representing CCCCO

(i) Lobbying federal, state, or local officials by Key Talent grantees/subgrantees including but not limited to, Deputy Sector Navigators, Sector Navigators, Regional Consortia Chairs, and Technical Assistance Providers, when using their "Key Talent" title, status, and CCCCO grant funding is strictly prohibited without Chancellor's Office permission. Lobbying activities include, but are not limited to:

(ii) Seeking to increase funding for a federal or state program; and

(iii) Influencing enactment or modification of any pending federal or state. Key Talent grantees shall obtain permission to lobby from a Workforce and Economic Development Division Vice Chancellor or dean in writing. A request must include the program and/or bill, purpose of lobbying activity, position on program and/or bill and basis for position, and how this activity would meet the goals of the grant.

Section 2.02 Program Management

(a) Requirements for Strategic Planning & Artifacts

(i) Grantee or subgrantee Program Managers, or an equivalent resource, will schedule and host a strategic planning session with Chancellor's Office Sponsors, Leads and Monitors 2 times annually, based on the following schedule:

1) By the end of May for the purpose of drafting the program/product/service roadmap, workplan and budget for the next fiscal year, and
2) By the end of November for the purpose of reflecting on accomplishments, to draft a mid-year progress report (due at the end of January) and revising the product/service roadmap, workplan and budget for the 2nd half of the fiscal year.
3) The Chancellor's Office Sponsors may elect to include other stakeholders as deemed appropriate.

(b) Other Expectations – Workplan and Budget Artifacts

(i) Within the RFA Response, and all associated performance reporting thereafter, must be represented a level of detail that allows Chancellor's Office representatives to draw alignment to the Project and Product Roadmaps, the budget assumptions as well as the project organization.

(ii) Any workplan and budget submitted by a grantee or a subgrantee to the grant monitor without completing the strategic planning process and obtaining the CCCCO sponsors' sign-off will be deemed invalid and will be returned to the grantee or subgrantee to properly complete the process.

(iii) *Grantees and subgrantees are required to submit a detailed budget, providing context about planned and actual expenditures. Details may include, but are not limited to, technology vendor name, employee and contractor names, project roles (e.g. project mgr.), project alignment, % allocation for shared resources, etc. As part of the detailed budget, grantees and Subgrantees should provide a payment schedule.*

1) Payment Schedules

The purpose of this effort is to ensure that grantees are able to manage their expenditures so that they are able to cover the cost of delivering on the services and solutions as written in this RFA and ultimately, the work plan. The objective is to ensure that grantee payment terms are structured in a balanced way so that grantees do not assume excessive financial risk and the CCCCO has full visibility into grant fund expenditures.

Please provide a payment schedule that includes the following categories of information:

a) Maintenance and operations (M&O) costs by month (includes corrective, adaptive, and perfective maintenance efforts) including:
   i) Software/Product/Tools (e.g., ongoing licensing, one-time acquisition implementation cost)
   ii) Staff costs
   iii) Vendor/contractor costs
   iv) Hardware (e.g., servers, network gear, workstations, laptops, other, and warranty/maintenance)
   v) Subscription Services (SaaS, PaaS, IaaS/cloud)
   vi) Other (e.g., travel, conferences, training, meetings)

b) Project/Initiative Costs by month (costs associated with defined projects; once these projects enter steady-state, these projects become part of M&O). For each project, include the following costs:
   i) Software/Product/Tools (e.g., ongoing licensing, one-time acquisition implementation cost)
   ii) Staff costs
   iii) Vendor/contractor costs
   iv) Hardware (e.g., servers, network gear, workstations, laptops, other, and warranty/maintenance)
   v) Subscription Services (SaaS, PaaS, IaaS/cloud)
   vi) Other (e.g., travel, conferences, training, meetings)

c) Date (mm/yyyy) when grantee will submit an invoice to the CCCCO (assume 60 calendar days for payment by CCCCO)

d) For all software/product/tools, vendor/contractor, subscription services, and other contracts, please include contractual payment terms

(iv) *When reporting budget performance, grantees and subgrantees will provide visibility to original budget, actual expenditures, and will outline explainable variance (+/-).*

(v) *If any unpaid, or unexpended funds remain at the end of any given fiscal year (surplus) due to the inability to fully complete a workplan objective, the grantee or subgrantee may carry-over the surplus into the workplan and budget for the next fiscal year with the prior approval of the CCCCO Sponsors during the May strategic planning session, and subject to grant term limits, confirmed CA budget amounts and BOG approval. In this case, the total amount of prior year carry-over objective and dollar amount must be clearly represented within the workplan and the budget detail for the next fiscal year.*

(vi) *The grantee or subgrantee Program Manager or equivalent, will provide CCCCO Sponsors, Leads and Monitors with read access to all program and project collaboration sites and artifacts.*

(c) Program Management Reporting Requirements

(i) All grantee or subgrantee program managers, or equivalent role, will be responsible for producing and distributing the following program level reports to the CCCCO Sponsors, Leads and Monitors:

1) Monthly program status summary, including accomplishments against objectives and milestones, milestones for the month ahead, critical risks and issues, and any action required from the CCCCO
2) Quarterly status summary, including financial performance summary (budget vs. actual + estimate to complete, estimate at completion (forecast))
3) Mid-year and annual report with budget narrative and summary, and explained variance

Section 2.03 Project Management

(a) Grantee and subgrantee project managers will engage with the designated CCCCO PMO functional lead, and adhere to CCCCO project management standards.

(i) In line with the CCCCO PMO framework, the following project artifacts (at a minimum) must be created and continuously updated by the project manager(s) for any in-scope projects:

1) A project dashboard (on PMO collaboration site)
2) A detailed project plan, a project organization chart, a RACI matrix (roles, responsibilities and decision authority) and a detailed resource forecast
3) A risk, decision and action item tracking spreadsheet
4) A budget tracking spreadsheet (project cost accounting)
5) A project status report summary presentation
6) Resource forecast, updated monthly, by resource type (FTE vs. Contractor/Consultant)

Section 2.04 Product Management

(a) Grantee and subgrantee program and product managers will engage with the designated CCCCO PMO functional lead, and adhere to the following CCCCO product planning and artifact standards:

(i) Product planning

1) Product Managers will support and participate in strategic planning activities in conjunction with the CCCCO Lead and the Program Manager to confirm the product strategy and long-range product roadmap.
2) Product Managers will be responsible for creating and maintaining product content which may be leveraged by the CCCCO for various architecture and product portfolio management activities, and product development team(s) over time. Product summary artifacts include, but are not limited to:
   a) Product strategy and system-wide strategic value (system and data)
   b) Functional capabilities and features by user group
   c) Workflow and user roles/permissions
   d) Data flow diagram
   e) Entity relationship diagram
   f) Data model
   g) Architecture diagram
   h) Product Roadmap (12-18 month, rolling)
   i) Release plan (12-18 month, rolling)
   j) Prioritized epic and user story inventory (sprint plan)

Section 2.05 Quality Assurance within the Software Development Lifecycle

(a) Grantees/Subgrantees developing or configuring technical solutions funded through the CCCCO will maintain a defect log by code-base or release, classified by impact and priority (high, medium & low). The defect log will be shared with the CCCCO and leveraged to manage quality and make go/no-go decisions through the development lifecycle.

(b) Additionally, the defect log will be reviewed to measure release quality 2 weeks post production deployment.

(i) A release to production will meet CCCCO quality standards if:

1) If 100% of the intended release package was deployed
2) Zero critical or high defects reported (either directly related to new features/functions, planned bug-fixes, or impact to existing functionality)
3) 2 or less medium defects reported, which can be resolved within 2 days

(c) The CCCCO Lead will be engaged by the project manager or product manager to:

(i) define user acceptance (UAT) test entry and exit criteria, and to assign UAT testers from represented user groups, and

(ii) attend a go/no-go meeting to confirm readiness and obtain sign-off to deploy to the production environment.

Section 2.06 Environmental Management

(a) Grantees/subgrantees developing or configuring technical solutions funded through the CCCCO will ensure a sufficient number of environments to support Agile development methodology and quality assurance practices, including but not limited to:

(i) Multiple configuration (sandbox), dev, test environments

(ii) A minimum of one production-like environment for use in end-to-end quality assurance testing, user acceptance testing and/or user training.

Section 2.07 Integrated IT Change Control

(a) As appropriate, Grantees and/or subgrantees will participate in an integrated IT Change Control process to increase visibility, tighten coordination and collaboration across edtech technical stakeholders, and reduce risk of adverse impact to stakeholders and other IT services and processes.

Section 2.08 Resource and Vendor Performance Management

(a) Grantees and subgrantees will actively set performance expectation, consistently track performance against expectation, and immediately remediate poor performance where necessary to ensure that grant objectives are met on schedule, on budget and with high quality. The grantee or subgrantee will notify the CCCCO Sponsors, Leads and Monitors if resource or vendor performance is below expectation.

Article III. Program Communications

(a) Newsletters & Press Releases

(i) *All system-wide announcements, newsletters and/or press releases developed by way of Chancellor's Office program grant funding and/or which contain information about a program or initiative funded by way of a Chancellor's office grant, will be submitted by the grantee or subgrantee to the CCCCO Sponsor(s), CCCCO Lead and CCCCO VC of Communication for review and approval.*

1) Please email an editable soft copy of final drafts 2 weeks (10 business days) in advance of the scheduled communication date, noting required action and response due in the email subject title.
2) If an unplanned communication must be delivered immediately, please flagged the email as urgent, and follow-up with the Grant Monitor and the Vice Chancellor via phone to provide context and prompt immediate action.

(b) Public Communications, Media Relations and Product Endorsement

(i) *Grantees/subgrantees and their employees, as well as contractors, working on behalf of the California Community Colleges Chancellor's Office, and public communications must all be consistent and in alignment with the priorities of the Chancellor's Office.*

1) All requests for media interviews must be approved in advance by the Chancellor's Office division of communications and marketing (or its designee) before an interview with a news organization, blog, trade journal or other publicly disseminated media publication is given.
2) The Chancellor's Office division of communications and marketing (or its designee) must approve all public speaking engagements at events that may garner media attention.
3) No press releases or statements from any initiative shall be issued unless approved in advance by the Chancellor's Office division of communications and marketing (or its designee).
4) Technology initiatives and their representatives shall not publicly endorse products. While vendor relations are an important function of grant administration and operations, the California Community Colleges does not publicly promote or endorse products. Doing so runs the risk that the California Community Colleges is perceived as currying favor with the vendors, which suggests a possible hidden agenda that undermines public trust.
5) Grantees may provide vendors with letters of reference, upon the request of the vendor, in connection with a vendor's response to a request for proposals. Such letters should be reviewed by the Chancellor's Office.

Article IV. Information Technology - Regulatory and Policy Standards

Section 4.01 Information Security

(a) Regulatory Basis

(i) *The Chancellor's Office adheres to federal and state laws concerning access to and confidentiality of student record information including the federal Family Educational Rights and Privacy Act (FERPA), as authorized by 20 U.S.C. §1232g(b) and 34 CFR Part 99; and California Education Code Section 76200, and utilizes National Institute of Standards and Technology (NIST) guidelines to protect sensitive information resources.*

(b) Personal Identifiable Information – Care and Due Diligence Expectations *(i) California Community Colleges Chancellor's Office (CCCCO) is responsible for ensuring that CCCCO data is protected appropriately and meets the needs and risk tolerance levels of the business by aligning with the guiding principles of the CCCCO and regulatory requirements. As a liable agency, CCCCO is responsible for ensuring its partners protect all Personally Identifiable Information (PII) with the same care and due diligence. Note: These requirements are subject to change based on revised legislation and industry trends.*

(c) Information Security Administrative Regulations Expectations

(i) All Grantees and subgrantees shall adopt, and comply with, the Chancellor's Office Information Security Administrative Regulations (ARs) and procedures.

1) Reference the Information Security Administrative Regulation Overview
2) Review the Information Security Administrative Regulations by category

(ii) All Grantee and subgrantee resources doing work funded by way of a Chancellor's Office program grant must complete the CCCCO Information Security Certification course during onboarding, which must be renewed annually thereafter.

(iii) Must take immediate action to adopt ARs and define a plan to implement standard practices and schedule information Security Certification training.

(iv) Please contact CCCCO Information Security Officer or Analyst for guidance and support.

(d) Secure Data Sharing Agreements

(i) CCCCO aggregates/disaggregates, compiles, analyzes, and reports college data for requests regarding, but not limited to, student enrollment, credentials earned, program parameters, graduation rates, success rates, and survey results. The Chancellor's Office is responsible for the protection of data assets relative to sharing data with internal and external entities. These responsibilities include the following:

1) ensure that only appropriate external entities are approved for access to unitary-level data;
2) execute memoranda of understanding or data sharing agreements, which includes the provision of non-disclosure agreements from individuals with access to the data;
3) designate a contact person to be responsible for oversight and supervision of the security and confidentiality of the data;
4) if necessary, make on-site inspections of external entities to ensure that the terms of agreements and all applicable laws and regulations are being met;
5) if an audit or on-site inspection reveals a violation of the terms of agreements or applicable laws and regulation, suggest corrective action, which may include terminating the agreement with the external researcher; and
6) in the event of a breach, follow all state-mandated procedures to minimize risk to student and employee records and the Chancellor's Office.

(ii) Grantees and subgrantees that will develop data sharing agreements, or require Chancellor's Office data to fulfill work funded by way of a Chancellor's Office program grant must take the following action:

1) Review the CCCCO Data Sharing Policy
2) Complete and submit the CCCCO Data Sharing Form
3) Contact CCCCO Data Manager for guidance and obtain the most recent versions of the policy and form.
4) Receive approval from the CCCCO for all MOU templates created subject to review, refinement and approval prior to presenting to internal or external parties for review and approval
5) Must have standard IP language reflected within Appendix A and Appendix E

6) Include a clause “subject to change based on CO strategy and/or legislation” within the draft MOU
7) Obtain CO officer signature(s) to be fully executed
8) All executed MOUs are to be uploaded to CO doc repository

(e) CCCCO Information Security Standards and Controls – Contract Addendum

(i) The following Information Security standards and controls must be implemented immediately within all in-flight Chancellor’s office grant funded programs and projects, and the following contract language must be included in all new RFAs, and grantee and subgrantee contracts going forward

(ii) Project Deliverables – Deliverables produced during the project must be reviewed in detail and must be approved by all project stakeholders. A signature page or section should accompany each deliverable requiring approval. The following is a listing of deliverables required of all projects:

1) System Development Document – establishes the hardware and network development approach including methodologies, tools, and procedures to be employed; also includes development procedures for issue tracking and configuration management and any other information that aids in the implementation of the system
2) System Document– integrated hardware, network, and/or firmware components that meet all requirements
3) Integration Document – describes the assembly and interaction of the hardware, network, and any other components of the system
4) Test Analysis Report(s) – presents a description of the unit tests and the results mapped to the system requirements; also identifies system capabilities and deficiencies
5) Conversion Plan – describes the strategies and approaches for migrating data from an existing system to another hardware/network environment. This document is only applicable for projects involving the migration of data.
6) Implementation Plan – describes how the information system will be deployed as an operational system
7) Operations Manual, Run Book or Systems Administration Manual – The Operations Manual focuses on mainframe systems; the Systems Administration Manual is oriented toward distributed (client/server) systems
8) Release Notes – provides summary information regarding the current release of the system being built; typically includes major new features and changes and identifies known problems and workarounds
9) Maintenance Manual – details effective system maintenance. Appendices might document maintenance procedures, standards, or other essential information.
10) Training Plan – outlines technical and user training needs on the new or enhanced information system
11) Security Scan Certification Report-provides assurance that client’s application is reliable and free from security issues

(f) Access Control – Local Authentication: When providing local user access to the client’s data, the vendor shall employ authentication for system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 2 or higher*. The following security controls are required:

(i) Mixed case (upper and lower case)

(ii) Alpha Numeric (numbers and letters)

(iii) *At least one special character (e.g., $, #, %, &, *)*
(iv) *Must be changed at least every 90 days*
(v) *Password may not be reused for 10 rotations*
(vi) *Limit the number of access attempts to 3-6 attempts before locking the account*
(vii) *Passwords are not stored in clear text*
(viii) *Passwords are not cacheable via frontend*
(ix) *Provide password requirement for both application users and staff accessing the data residing at vendor and system administrators (internal controls)*

(g) Access Control – Remote Authentication: When providing a remote user access to the client's data, the organization shall employ multifactor authentication for system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3 or level 4. (e.g. Two Factor Authentication). The following security control is required:

(i) 2-factor authentication at vendor's site (vendor's staff accessing vendor's database)

(h) Access Control – Role Based Access: The organization shall provide secure role-based account management. Privileges will be granted utilizing the principle of least privilege. The following security controls are required:

(i) *No shared accounts exist or allowed.*
(ii) *There is an assigned staff admin to create/delete accounts.*
(iii) *Only "minimum required" privileges are granted to the users.*
(iv) *There is accountability for deleting user accounts upon user's termination.*
(v) *There are different roles for different users.*
(vi) *Each vendor must document how user roles are defined and administered. Common user accounts and roles include, but are not limited to the following:*

1) Local Admin Accounts
2) Privileged User Accounts
3) Domain Admin Accounts
4) Emergency Accounts
5) Service Accounts
6) Application Accounts

(i) Access Control – Session Termination: The information system automatically terminates or locks a remote session after the organization-defined time period of inactivity requiring user re-authentication. The following security control is required:

(i) *Inactive session will terminate in less than 30 minutes*

(j) Access Control – Connecting to sensitive and confidential from non-company assets: For remote connectivity, the vendor must require their workforce members to only use company owned workstations / laptops to connect to any system which houses the client's data. The following security control is required:

(i) *The vendor must prohibit remote connections from non-company owned laptops or workstations (e.g., personal laptops and workstations, mobile devices)*

(k) Audit and Accountability – Auditable Events: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. (e.g. user authentication, access to data, modification of data). The following security controls are required:

(i) User Name
(ii) Last login time of the user
(iii) Records that are accessed/viewed by the user
(iv) Records that are modified by the user
(v) Records that are deleted by the user
(vi) Duration of the active session
(vii) User creating a new record/table/database
(viii) User copying/duplicating a table/database

(l) Audit and Accountability – Analysis and Reporting: The organization regularly* reviews/analyzes audit records for indications of inappropriate or unusual activity. The organization investigates suspicious activity or suspected violations. (e.g.; logs are reviewed daily; suspect activity is immediately investigated). Applicable if the vendor is hosting the data. The following security controls are required:

(i) Critical events are reviewed by Vendor daily
(ii) Critical events are analyzed and acted upon in a timely manner

(m) Media Protection – Media Storage: The organization protects portable information system media (e.g. Laptops, Backup tapes, USB thumb drives, CD/DVD, etc.) containing sensitive or confidential information with an appropriate cryptographic mechanism. The following security controls are required:

(i) Data on local machines that process sensitive or confidential information must not be cached (e.g.., temp files)
(ii) All laptops and removable store must be encrypted at all times
(iii) Sensitive or confidential data must be encrypted at column level for all critical data in the database
(iv) System backups must be encrypted

(n) Media Protection – Sanitization and Disposal: The organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse. The following security controls are required:

(i) Digital media (hard disks, tapes, discs, USBs, etc.) must be appropriately destroyed using DOD standards
(ii) Digital media (hard disks, tapes, discs, USBs, etc.) if not destroyed must be degaussed using DOD standards prior to reuse
(iii) Papers with sensitive or confidential information must be destroyed using cross-cut shredders

(o) Physical Protection – Visitor Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides. The following security controls are required:

(i) System/database containing sensitive or confidential data must be physically protected

(ii) Visitors are properly identified at the visit datacenter / server room (including time of entry/exit) and are accompanied by staff

(iii) Alarms and cameras are present at the datacenter

(iv) Badges and equipment checks are in place for personnel who need access to the datacenter or server room

(v) The datacenter has security staff/guards 24x7

(p) Personnel Security – Screening: The organization screens individuals requiring access to sensitive or confidential information prior to authorizing access. The following security control is required:

(i) Criminal background checks are conducted on all vendor staff with access to the client's data

(q) Personnel Security – Termination: The organization terminates information system access upon termination of individual employment. The following security controls are required:

(i) Network access must be removed immediately upon termination of vendor's staff

(ii) Application access must be removed immediately upon termination of vendor's staff

(iii) All assets (laptops, phones, etc.) returned to vendor immediately upon termination of vendor's staff

(r) Risk Management – Vulnerability Assessment: The organization scans for vulnerabilities in the information system at least annually. The following security controls are required:

(i) Vendor's database and other critical systems are periodically scanned by a vulnerability scanning tool

(ii) Vendor uses an application scanner to certify the application is free of security issues

(iii) Prior to the deployment, the vendor will provide certification at the end of the project

(iv) The vendor will provide a yearly certification for the application that it is free of security issues

(s) System and Communication Protection – Application Partitioning: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). The following security controls are required:

(i) Database, application and web servers must be logically separated

(ii) Database, application and web servers must be physically separated

(t) System and Communication Protection – Boundary Protection: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. (e.g., firewall between internet facing servers and the internal network). The following security controls are required:

(i) Database and application servers must be protected by firewalls

(ii) Critical systems (internal network) must be protected by firewalls

(u) System and Communication Protection – Transmission Confidentiality: The information system employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measure. The following security control is required:

(i) Data must be encrypted using during transmission

(ii) Encryption used must be industry best practice

(v) System and Information Integrity – Flaw Remediation: The organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe (e.g., deployment complete within 30 days from security patch release). The following security controls are required:

(i) Critical patches must be applied within 30 days for all vendor systems, including:

1) operating systems
2) 3rd party application (e.g., Adobe)
3) Applications

(ii) Monitoring tools must be in place to track and report the patching levels of all systems

(w) System and Information Integrity – Malicious Code Protection: The organization employs malicious code protection mechanisms at critical information system entry and exit points, and at workstations, servers, or mobile computing devices to detect and eradicate malicious code (e.g., antivirus on mail gateways). The following security controls are required:

(i) Anti-malware/anti-virus software must be present on all vendor systems (workstations, servers, etc.)

(ii) A formal IT Change Management process must be in-place for any changes to the critical system(s)

(x) System and Information Integrity – Monitoring Tools and Techniques: The organization employs tools and techniques to monitor events on the information system to detect attacks, and provide identification of unauthorized use of the system (e.g., intrusion detection systems (IDS), intrusion prevention systems (IPS), audit record monitoring software, network monitoring software). The following security control is required:

(i) IDS/IPS must *be in place to protect Vendor's network*

(ii) *IDS/IPS must be industry best practice*

(y) IT Change or Configuration Control – Protecting system and information integrity: The organization employs tools and techniques to allow only authorized changes to be introduced into the production environment and prevents unauthorized changes to production systems through restriction of privileged access accounts, and detects unauthorized changes through periodic review of system and data access. The following security controls are required:

(i) The vendor must have a IT Change Management or Configuration Control policy

(ii) The vendor must conduct regular reviews of all changes prior to making changes to the production system

(iii) The vendor must adhere to "separation of duties" for all accounts related to changes on the production systems

(z) Business Continuity/Disaster Recovery Planning – Contingency plans and regular testing: The organization has documented procedures for contingency operations to ensure continuous operation. The contingency plans are subject to regular update and review and are tested on a periodic basis. The following security controls are required:

(i) *Organization must have a current BCP/DRP policy and documented procedures*

(ii) *Application/service critical (must have immediate recovery within 24-48 hours prior to effecting our student or college). Check messaging and sentence structure*

(iii) *The vendor must review and update their contingency plans on a regular basis (at least once every 2 years)*

(iv) *vendor conducts periodic testing (at least once every year) of the recovery plans with the client*

(aa) Incident Response – Reporting Criteria and Standards

(i) *Grantees and subgrantees engaged in technology projects funded by way of a Chancellor's office grant, must immediately report information security incidents to the CCCCO Information Security Team based on the following criteria and standards:*

(ii) *Information Security Incident Criteria*

1) An information security incident is an occurrence that:

a) Actually, or potentially jeopardizes the confidentiality, integrity, and/or availability of an information system or the information the system processes, stores, or transmits, or

b) Constitutes a violation, or the imminent threat of violation, of information security standards, policies and procedures

(iii) *REPORTING Standards*

1) Incidents which must be reported to the California Community College's Chancellor's Office immediately following discovery include, but are not limited to, the following:

a) Data (includes electronic, paper, or any other medium) –

i) Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal

ii) Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29

iii) Deliberate or accidental distribution or release of personal information by an entity, or its personnel in a manner not in accordance with law or policy

iv) Intentional non-compliance by the custodian of information with his/her responsibilities

b) Criminal Activity – Use of an information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502

i) Unauthorized Access – This includes actions of entity personnel and/or unauthorized individuals that involve tampering, interference, damage, or unauthorized access to an entity's computer data and computer systems

ii) Attacks – This includes, but is not limited to, successful virus attacks or exploited vulnerability, web site defacements, and denial of service attacks

c) Equipment – This includes theft, damage, destruction, or loss of entity-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data

d) Inappropriate Use – This includes the circumventing of information security controls or misuse of an entity's information asset by entity personnel and/or any unauthorized individuals for personal gain, or to engage in unauthorized peer-to-peer activity, obscene, harassing, fraudulent, illegal or other inappropriate activity

e) Outages and Disruptions – This includes any outage or disruption to an entity's mission critical systems or public-facing web applications lasting more than 2-hours, or in which the incident triggers the entity's emergency response or technology recovery

f) Any other incidents that violate an entity information security or privacy policy

(iv) INCIDENT NOTIFICATION

1) CCCCO policy requires entities to make notification following discovery of an incident. Each entity's Chief Information Officer (CIO), Information Security Officer (ISO), or the assigned incident reporting personnel, collectively hereinafter referred to as "the reporter," is responsible for notifying CCCCO project stakeholders following these steps:

IMPORTANT**:** The Reporter should attempt to gather the following information. However, if the information is not available, notification should not be delayed.

a) Name and address of the reporting entity

b) Name, address, e-mail address, and phone number(s) of the reporting person

c) Name, address, e-mail address, and phone number(s) of the ISO

d) Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.)

e) Description of the incident

f) Date and time the incident occurred

g) Date and time the incident was discovered

h) Make / model of the affected computer(s)

i) Was the asset encrypted?

j) IP address of the affected computer(s)

k) Assigned name of the affected computer(s)

l) Operating system of the affected computer(s)

m) Location of the affected computer(s)

n) Actions taken prior to reporting the incident to CCCCO

Section 4.02 Information Security Audit Expectations - Software, Software-as-a-Service, and System Integration Partners

(a) Secure Design and Development:

(i) The Chancellor's Office provides security guidelines and protocols for software development and system integration partners that create software tools and services on behalf of the CO. The software development partners must abide by the CO's security protocols and accept periodical security audits performed by the CO or CO's contracted agents. These guidelines and audits are not meant to partially or wholly replace or supplant the software partner's responsibility and liability in ensuring the security and confidentiality of the tools they have created, the data they have stored, and the interfaces to other systems and data sources to which they may have access.

(b) Secure data transfer and integration:

(i) The Chancellor's Office is piloting services that enable more robust integration between systems and data services offered at the colleges and the systems and services hosted locally or remotely on behalf of the Chancellor's Office. The CO will provide best-practices guidelines, workshops, and technical assistance to the colleges in the implementation of these interfaces. The CO will also reserve the right to provide periodical security audits on these interfaces. The security measures provided and exercised by the CO are not meant to partially or wholly replace or supplant the colleges' responsibility and liability in ensuring the security and confidentiality of their systems, their data, and the interfaces with the CO.

Section 4.03 Accessibility – Information Technology

(a) Regulatory Basis:

(i) The Chancellor's Office adheres to federal and state laws concerning Accessibility including Section 508 of the United States Workforce Rehabilitation Act and CA Government Code 7405, Div.7, Title1, Chapter 18.1 and follows Web Content Accessibility Guidelines (WCAG) 2.0, Level A and Level AA standards for websites, web-based applications, and other electronic content (email communications, PDFs, Word documents, etc.). All Chancellor's Office grantees and subgrantees configuring or developing custom IT solutions shall adopt, and comply with, the Chancellor's Office Accessibility standards and protocols for information technology. All commercial technology Suppliers shall warrant that their products and services comply with the Chancellor's Office Accessibility standards and protocols.

(b) Compliance Warranties

(i) All grantees and subgrantees engaged in technology projects funded by the Chancellor's office shall provide credible, third-party verification demonstrating compliance of product accessibility per current requirements of the revised US Section 508 Standards and Web Content Accessibility Guidelines 2.0, Level AA (WCAG 2.0, AA) upon initial deployment and with each major subsequent release prior to production use by faculty, staff, or students. Appropriate documentation detailing the testing, including evaluation results, will be current and maintained.

(ii) All technology Suppliers must warrant that their software, products and services adhere to Section 508 of the Rehabilitation Act of 1973 and is fully compliant with WCAG 2.0 AA-Level standards for accessibility. Credible verification and/or documentation regarding the accessibility of the software, product, or service will be provided by the Supplier upon request.

(c) Accessibility - Non-compliance

(i) If portions of the software, software-as-a-service, or user experience are discovered to be non-compliant at any point, the Chancellor's Office, or its' authorized agents, will notify Supplier immediately. If any student accommodation is found to be necessary due to an identifiable lack of accessibility in the Supplier software, the cost for accommodation will be paid by Supplier upon request by the Foundation, once verified that the student accommodation conforms with Section 508 of the Rehabilitation Act of 1973 and that the noncompliance did not arise from intermediary interference (e.g., virus protection software, web browser problems, or out of date assistive technology) or a student's inability to properly utilize compliant assistive technology.

1) If necessary, an independent and mutually agreed upon, 3rd party accessibility firm may be used to validate the lack of software accessibility. Reasonability of cost for accommodation will be upon mutual agreement by Supplier and the Chancellor's office or their authorized agents.

(d) Accessibility Advisory Support and Services – Chancellor’s Office vs. Locally Funded Initiatives

(i) To limit the Chancellor’s Office risk exposure, grantees or subgrantees <u>shall not</u> provide technology Accessibility advisory and/or assessment services to Districts or Colleges for technology projects, solutions and/or work products which are funded locally through CCC Districts and Colleges, and not by way of a Chancellor’s Office program grant. In this regard, Accessibility advisory services include, but are not limited to the following:

1) Design and development standards and techniques for mobile, web and desktop applications, and/or other digital content
2) State and Federal Accessibility code of regulation and/or regulatory compliance risk management protocols

(ii) Grantees and subgrantees shall refer representatives of locally funded technology projects or work products to the Information Technology and Human Resource leaders within the funding District or College, and may provide the link to <u>WC3 Web Content Accessibility Guidelines 2.0</u>, which is the standard framework leveraged by the Chancellor’s Office.

(e) Accessibility Advisory Support and Services – Online Education

(i) The Chancellor’s Office is providing Course/Learning Management Systems for the colleges in the form of Canvas and the Online Exchange. The Chancellor’s Office and/or its authorized agents, may provide Accessibility-related best-practices guidelines, course templates, workshops, and technical assistance for the colleges. The colleges must continue to work with their faculty and staff to honor the academic freedom rights of their faculty while concurrently complying with state and federal accessibility laws. These accessibility practices must exist for courses offered locally at the colleges and the courses offered by the colleges through the Online Exchange. The accessibility support and guidelines provided and exercised by the CO are not meant to partially or wholly replace or supplant the colleges’ responsibility and liability in ensuring the accessibility of each and every course they offer on campus, locally online, or through the Exchange.

Article V. Intellectual Property and Contract Termination Protocol

Section 5.01 Intellectual Property - Custom Code, Customized Configurations, and Data Assets

(a) All custom software code, custom analytic models and dashboards, custom processes and/or integrations, customized Commercial-Off-The-Shelf (COTS), Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and/or Infrastructure-as-a-Service (IaaS) configurations, and associated data sets and documentation developed as work products through Chancellor’s Office grant funding are considered the intellectual property of the Chancellor’s Office, regardless of contracted hosting party and/or hosting location.

Section 5.02 Intellectual Property - Contract Termination Protocol

(a) If notification to terminate contract is provided by any party, the Chancellor’s office will coordinate with the grantee or subgrantee to plan the successful migration of custom code, configurations, associated infrastructure, data sets and documentation, and complete knowledge transfer sessions, prior to the negotiated contract termination date.